

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

STEVEN G. MILLETT,)	
MELODY J. MILLETT, et al,)	
)	
Plaintiffs)	
)	
vs.)	C. A. No. 05-599-SLR
)	
TRUELINK, INC.)	
A Trans Union Company,)	
Defendants)	

EXPERT'S REPORT, ROBERT ELLIS SMITH

I, ROBERT ELLIS SMITH, provide the following Expert Report pursuant to the Federal Rules of Civil Procedure in connection with this action:

BACKGROUND AND QUALIFICATIONS

Robert Ellis Smith is a journalist who uses his training as an attorney to report on the individual's right to privacy. Since 1974, he has published Privacy Journal, a monthly newsletter on privacy in a computer age. Based in Providence, R.I., it is the world's longest-running publication in the field.

Smith is a frequent speaker, writer, and Congressional witness on privacy issues and has compiled a clearinghouse of information on the subject: computer data banks, credit and medical records, the law of privacy, the credit-reporting business, theft of identity, the federal Privacy Act, and physical and psychological privacy. Since 1974, he has reported on abuses of Social Security numbers and on the credit-reporting business. In the early 1990s, along with The San Francisco Chronicle, he was the first to report on theft of identity and to give the criminal activity that name.

Smith is the author of Our Vanishing Privacy (1993) and The Law of Privacy Explained (1993), as well as Privacy: How to Protect What's Left of It (1979); Workrights (1984), a book describing individual rights in the work place; Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet (2004). He is the editor of Compilation of State and Federal Privacy Laws (1976-2006), Celebrities and Privacy, and War Stories, a collection of anecdotes on privacy invasions.

Frank J. Williams, Chief Justice of the Rhode Island Supreme Court, praised Smith's "balanced viewpoint," saying, "We deal with so many people who are not exactly rational about their point of view. I respect that he's not like that" [Rhode Island Law Tribune, September 10, 2001].

The New York Times said Smith "sounds the alarm about maintaining freedom and privacy in the computer age" and called him "a principled critic." Privacy Journal is "a privacy watchdog," according to Time, and "the paper of record for lawyers and others interested in privacy rights," according to U.S. News and World Report.

Smith has twice been asked to write the definition of privacy for the World Book Encyclopedia.

A 1962 graduate of Harvard College, Smith received his law degree from Georgetown University Law Center in 1976. From 1970 to 1973, Smith was the assistant director of the Office for Civil Rights in the U.S. Department of Health, Education, and Welfare. Prior to that, he had nine years of experience as a news reporter and editor.

He served as a member of the District of Columbia Human Rights Commission until 1986. From 1991 to 1992 he served as a Special Assistant to the Attorney General of Rhode Island, investigating the collapse of several of the credit unions in the state. Between 1992 and 2000, he served as vice chair of the R.I. Coastal Resources Management Council, which restricts development on the state's 600 miles of coastline.

Smith is an attorney in the state of Rhode Island. He is also licensed to practice in the District of Columbia and has been a member of the American Bar Association privacy committee.

Smith has been an expert witness on privacy before the U.S. House Subcommittee on Government Information 1974; Senate Subcommittee on Consumer Affairs 1975 and 1980; Senate Subcommittee on the Constitution 1977; House Subcommittee on Courts, Civil Liberties, and the Administration of Justice 1984; House Subcommittee on Consumer Affairs 1989; House Ways and Means Subcommittee on Social Security 1991; state legislative committees in Florida, Indiana, Iowa, Kansas, Massachusetts, Michigan, Rhode Island, Utah, and Washington State; and the White House Commission on Aviation Safety and Security in 1997. In 2000 he gave the keynote address on theft of identity at the annual meeting of the National Association of Attorneys General, and in 2001 he addressed the annual meeting of the National Association of Chief Justices, on the dangers of personal information, like Social Security numbers, on court Web sites.

He was the only privacy advocate to participate in the Federal Trade Commission meeting in November 1996 that led to development of the commission's Web site on identity theft and its responsibility to aid victims. Since 1992 he has advised victims of identity theft about remedies and has attended between six and ten national conferences on the subject.

In its publication of the results of an opinion survey it sponsored, "Equifax Report on Consumers in the Information Age" (Atlanta, 1990), on page iv, Equifax Inc., one of the three major credit bureaus, listed Smith among eight "Experts on Privacy" and acknowledged his advice.

In 2000, Trans Union, parent company of TrueLink, invited Smith to Tucson, Arizona, to address its senior executives on consumer expectations in privacy protection.

PRIOR LITIGATION TESTIMONY AS AN EXPERT WITNESS

Since 1985, Smith has given testimony by deposition or trial in 12 cases in federal and state courts. His four most recent cases are:

Coleman v. Trans Union, CA4:98CV169B-B (N.D. Miss 2002), jury verdict for plaintiff (failure to correct credit information) (t). Plaintiff's attorney: Sylvia M. Antalis, Sandusky, Ohio, 419/624-3000.

Remsburg v. Docusearch, Inc., CA C-00-211-B (D. N.H.) settled 2004 (negligent disclosure of personal information by a World Wide Web site) (d). Plaintiff's attorney: David M. Gottlesman, Nashua, N.H., 603/889-5959, dgottlesman@nh-lawyers.com.

Beaven v. U.S. Department of Justice, CA No. 03-84-JBC (E.D. Ky), judgment for defendants 2004 (negligent disclosure of Social Security numbers belonging to federal prison employees). (d). Plaintiff's attorney, Douglas McSwain, Lexington, Ky., 859-255-8581, dmcswain@sturgillturner.com

Thomas v. Smith, 97-7159-CI-21 (Cir. Ct. Pinellas Co., Fla.), pending, trial held Nov. 20, 2006 (challenge to the state's demand for Social Security number to qualify for homestead exemption in residential real estate taxation) (t). Plaintiff's attorney, Michael Hooker, Tampa Fla., 813/229-3333, gmconnell@glennrasmussen.com.

(d) = Deposition testimony

(t) = Trial testimony

FEE

My fee is \$200 per hour, plus travel expenses.

SCOPE OF MY WORK IN THIS MATTER

In connection with my work in this case, I have reviewed the Fourth Amended Complaint and Corresponding Answer, the Agreed Protective Order, copies of pages said by named plaintiffs to be from TrueLink's Web site, and a list of documents in the case from the plaintiffs' attorney. I may review additional materials as requested. I expect also to review materials in my possession, including back issues of my publication, Privacy Journal; my files on identity theft and abuses of Social Security numbers, public-opinions surveys, monographs, the FACTA report referenced below, and government reports in my possession, and cases on identity theft. I will

rely on my experience as a journalist gathering information about identity theft and privacy, at national conferences, trade association meetings, law enforcement meetings, consultations, and interviews with victims, law enforcement, credit-bureau officials, and other sources.

EXHIBITS

I expect at this time to present no exhibits.

OPINIONS TO BE EXPRESSED

I am prepared to testify about the process of theft of identity and how it works, commonly accepted definitions of identity theft, the practices and procedures in the credit-reporting business, the use of consumer credit reports in our economy, characteristics of the Big Three credit bureaus, and the crucial role of Social Security numbers in this process. I am prepared to testify about the negative consequences to victims and potential victims of identity theft, as well as the expectations of most consumers when enrolling in a Web-based "credit-monitoring" or "identity-theft monitoring" service. I counsel persons victimized by invasions of privacy, and I compile and publish an annual collection of stories involving such persons.

For more on the operations of the credit-reporting industry, see Report to Congress Under Sections 318 and 319 of the Fair and Accurate Credit Transactions Act of 2003 (Federal Trade Commission, December 2004). FACTA is the popular name for amendments to the Fair Credit Reporting Act in 2003.

These views are based on 27 years of experience (1) as a journalist monitoring business practices through news reporting, attending conferences, interviewing participants, and responding to consumers' complaints; (2) as an attorney researching case law and administrative law, lecturing on the subject, testifying before legislative groups, and assisting other attorneys in litigation; and (3) as an author of authoritative books and special reports on privacy and issues related to credit-reporting.

This phenomenon involves (1) a stranger misappropriating a person's "credit identity" and amassing hundreds of dollars in fraudulent credit charges, or (2) an undocumented immigrant misappropriating an innocent person's identity, or (3) a stranger using certain elements of an innocent person's identity for whatever reasons, including criminal activity. (A new variation is called "medical identity theft," in which an impostor gains medical treatment in the name of an innocent victim. There is also identity theft committed in bankruptcy proceedings.) A characteristic of the crime seems to be that it is committed in localities far away from the residence of the victim. It is committed by organized criminal rings and by individuals acting alone.

The first variety of identity theft cannot be committed without access to a person's Social Security number. It is important to realize that the crime can be committed with nothing more than a person's Social Security number and name. Theft of identity does not generally originate with stolen wallets or lost credit cards; 90 percent of it originates through access to Social

Security numbers stored by businesses and government agencies, according to Trans Union's own data. [Privacy Journal, Feb. 1996, p. 4].

In Ben Franklin's Web Site, a history of privacy and information collection in the U.S., I provided this description:

By the 1990s . . . it was called 'identity theft.' A stranger would secure the victim's Social Security number – from payroll records, by pretext over the telephone, in trash cans, or at World Wide Web sites – and then pose as that person to get a duplicate birth certificate, driver's license, or job. In a more common variation, the impostor would access the individual's credit report – using the Social Security number to verify identity – and discover the retail credit accounts the person had and the account numbers. Then the stranger would ask the retailers to change the address on the account to the impostor's or to a bogus address set up for this purpose. Or the impostor would simply use the victim's Social Security number to apply for a new account. The victim would be unaware that a stranger was using the accounts to order products and services – dunning notices for overdue accounts would be sent to the impostor's new address, not to the true account holder's address. But notices about the delinquent accounts would be sent regularly to the major credit bureaus. Only when the individual was rejected on a new credit application or had credit cards canceled would he or she become aware of the fraud.

But then reclaiming a clean credit report became impossible. A credit bureau would dutifully erase the bad information as required by the federal Fair Credit Reporting Act of 1971, but in the next 45 days, when retailers and credit-card issuers would make their next automated reports to the credit bureau, the fraud-produced information would reappear on the victim's credit report. Only after Congress tightened the law in 1996 and the credit bureaus faced several lawsuits did they take partial steps to prevent this from happening over and over. Further, because retailers accepted the losses as a cost of doing business, they didn't bother to change their practices so that the fraud could be curbed. They didn't bother to alter their systems so that Social Security numbers were unnecessary to retrieve data about an individual.

A prime source of other persons' Social Security numbers is the identifying information at the top of a credit report, what the credit bureaus call "header" or "above-the-line" information, including phone numbers, addresses, mother's maiden names, and Social Security numbers. Because most people provide their telephone numbers on credit applications whether or not their numbers are "unlisted," credit bureaus include listed and unlisted phone numbers "above the line." The Federal Trade Commission, which regulates credit bureaus, ruled in a non-public negotiation in 1993 that credit bureaus are free to rent "header" information all they want. That is when identity fraud became a nationwide epidemic.

This means that "information brokers," which buy personal information from large vendors and resell it to individuals and small businesses, could easily purchase Social Security numbers and unlisted telephone numbers. Many of these brokers sold the data on their World Wide Web sites.

The Federal Trade Commission has compounded the problem by encouraging credit bureaus to use Social Security numbers to verify the identity of a consumer who seeks to

get a copy of his or her credit report, as permitted by law. A Social Security number does not provide much verification of a person's identity if a stranger can get it easily.

The irony is that two of the three major credit bureaus, Trans Union and Experian, offer for-profit services intended to alert consumers to the possibility of theft of identity involving their credit reports; yet the same credit bureaus are the cause of 60 percent of identity theft because they continue to use a Social Security number (even if the name or address do not match) to confirm a match between a credit inquiry from a credit grantor and a credit file in their databases.

It is true that a service like TrueCredit cannot possibly "monitor" all or even most instances of identity theft. Many instances do not involve fraudulent manipulation of credit reports at all; a credit bureau like Trans Union would be unaware of them.

(No service, however thorough, can provide "complete identity theft protection." No service can effectively guarantee a consumer, "Don't worry about your credit.")

A monitoring service affiliated with a major credit bureau ought to be able to monitor credit identity theft, because it has access to credit reports stored by the Big Three. Since 1996, the three major credit bureaus have claimed the ability to detect and flag fraudulent activity in a credit record. [Privacy Journal, February 1996]. TrueLink did not do even that in this case.

TrueLink, in its Web advertising, promises to procure "credit reports" (plural) and to access "one or more of the major credit bureaus." In my opinion, this leads a reasonable consumer to believe that TrueLink will at least alert him or her to instances of credit identity theft, and will monitor activity in more than one credit bureau to do so.

I am prepared to offer commonly accepted definitions of identity theft, including those in state statutes enacted in the past three years.

In 2001 the Federal Trade Commission, which regulates credit bureaus, Internet privacy, credit repair, and deceptive business practices and is charged by law to aid victims of ID theft, had this to say:

"An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name." ["ID Theft: When Bad Things Happen to Your Good Name," July 2001, Federal Trade Commission, p. 1]

In my experience, that coincides with the commonly accepted description of identity theft by the general public. See Remsburg v. Docusearch, Inc., 149 N.H. 148 (2003). Several states have enacted statutes on identity theft with definitions that coincide with commonly accepted lay perceptions.

In its Web site, www.ftc.gov/idtheft, the Federal Trade Commission says:

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Thus, identity theft is not limited merely to fraudulent use of consumer credit.

In many varieties of ID theft, the fraud artist first procures the name and/or Social Security numbers of victims, often from payroll or personnel records where the perpetrator either has access or knows an acquaintance who has access. A large number of these crimes begin with access to personnel records. The perpetrator then discovers the credit accounts that the individual has, by procuring a credit report. (The Fair Credit Reporting Act permits an individual to get a copy of his or her own credit report; the Federal Trade Commission, which enforces the act, encourages credit bureaus to use a Social Security number to determine whether the requester is who he or she claims to be.) Then the perpetrator asks creditors to change the address on the account. How does he or she verify his or her “identity”? By presenting the Social Security number of the victim. If the SSNs match, a credit bureau or a creditor assumes that it is dealing with the true individual.

The perpetrator then charges products and services, often by telephone or on-line, using his or her “drop” address (often a vacant lot) and the victim’s credit card number. Because the credit-card bill is mailed to the suspect’s address, the victim often does not discover that he or she has been victimized until long after the crime.

This fraudulent activity creates bills that are not paid. These delinquencies are reported by retailers to credit bureaus. The victim’s credit report is increasingly filled with delinquencies on accounts that he or she has, plus charges on accounts that he or she has never had. Again, because an individual has not recently applied for credit, he or she remains unaware of the identity theft.

Once an individual discovers the fraud, he or she seeks first to correct the fraudulent entries. It can take several months and continual letters and telephone calls to the three major national credit bureaus. Once the fraudulent information is deleted from the victim’s credit report (as required under the Fair Credit Reporting Act), a credit grantor will report the fraudulent information again in its next reporting cycle, usually 30 days. Thus, the bad information reappears on the individual’s credit report.

The first consequence of this, of course, is that an individual will not qualify for routine consumer credit applications. But the consequences go far beyond that:

(a) Most credit-card issuers terminate customers in good standing with them if random checks with a national credit bureau uncover delinquencies with other creditors or indications that the customer may be over-indulging in credit expenditures. (Many persons first discover that they are victims when their credit accounts in good standing – or their spouses’ – are terminated.)

(b) Credit reports are used by landlords.

(c) Credit reports are used by mortgage lenders and automobile lenders.

(d) Credit reports are also used by insurance companies to determine eligibility for life, home, or health coverage.

(e) Credit reports are used to determine eligibility for employment.

(f) Credit reports are used to determine eligibility for government benefits.

(g) Credit reports – presumably via a court order – are used by law enforcement agencies as leads in criminal investigations.

(h) The Department of Homeland Security proposes using credit reports to determine whether air passengers should be singled out for increased security checks at airports.

Thus, a negative credit report created by a case of identity theft can effectively cripple an individual's participation in the American economy. There is ample reason for a person, whether sophisticated or not, to fear becoming a victim of ID theft or to fear even the possibility of being a victim once sensitive personal information is disclosed.

These are only the economic consequences. The emotional consequences are as traumatic. A subset of the first type of identity theft mentioned above occurs when the stranger gets a job using the victim's identity. Or, on several occasions the stranger has been caught in the process of committing a crime with the innocent person's identity documents on his person or he has left the innocent person's documents at the scene of a crime.

In my opinion, the claims made on the Web site of TrueLink (Trans Union) are particularly tempting for a consumer because they are part of a pattern by credit bureaus to deceive consumers. The Big Three credit bureaus have been cited by the FTC for confusing the public about "free credit reports," about the content of "header" information in a credit report, about the meaning of "inaccuracies," the differences between credit reports and consumer-investigative reports." The promise to provide "toll-free credit specialists" is particularly disturbing because Trans Union and its two competitors have a history on not answering toll-free numbers in a timely way and providing trained personnel. They have been forced by statute – to create toll-free phone services and to "provide trained personnel [live persons, not machines] to explain to the consumer any information furnished to him pursuant [to the Fair Credit Reporting Act]. [15 U.S.C. 1681, sec. 610(c).] They had to be required by statute to disclose their toll-free telephone numbers to the public.

The industry has a long history of inaccuracy in its credit reports, with estimated inaccuracy rates in as high as 20 to 30 percent of its credit reports [Government Accountability Office, Report GAO-05-223, Credit Report Literacy, March 2005, finding 18 percent of consumers disputed the accuracy of their credit reports]. [See also Federal Reserve Bulletin, February 2003, at 48 et seq. and Privacy Journal January 1990 and August 1998.] According to the industry's own trade association, more than 20 percent (12.5 million) of all credit reports

examined by consumers themselves require a reinvestigation for claimed inaccuracies [CDIA Communications January 12, 2005]. This makes TrueLink's promise to allow a customer to "immediately find out about credit report changes including fraudulent activity, new inquiries, new accounts, late payments and more" specious.

TrueLink's claim that its monitoring service is "award-winning" is specious. (Trans Union, the parent company, also claims that its Web site is "award-winning." I have been unable to get Trans Union to disclose the source of this "award." I am unaware of any such source, after 33 years of monitoring this industry.

By contrast, Trans Union was awarded "a lifetime menace" award as a threat to privacy in 2002. The "Big Brother Award" is selected each year by the London-based group Privacy International after nominations from privacy specialists and advocates like myself. Privacy International presented me the more positive Louis Brandeis Award for privacy excellence in the same year.

The award-winning claim, in my mind, diminishes the credibility of the TrueLink Web site and bolsters the deception of the consumer.

In my opinion, the claims made by TrueLink to its prospective customers is so deceptive as to constitute a common-law breach of contract, to violate the principles of most state consumer-protection laws, as well as of the federal laws on deceptive advertising and unfair trade practices administered by the Federal Trade Commission, as well as the FTC's principles on deceptive Internet business practices.

This is my opinion because

(1) no one entity can provide "complete identity theft protection";

(2) no entity that limits its monitoring to credit reports can alert consumers to, much less protect them from, the usual forms of identity theft;

(3) TrueLink cannot rely on the accuracy of the credit records held by its parent, Trans Union, (Trans Union has a history of resisting consumer demands for accuracy, access, free credit reports, and protection from identity theft; and the Trans Union and its two competitors have been unable or unwilling to take feasible steps that would mitigate the theft of identity epidemic.

I declare under the penalty of perjury that the foregoing is true and correct.

Submitted this 30th day of July 2007,

Robert Ellis Smith

Robert Ellis Smith
P.O. Box 28577
Providence RI 02908
401/274-7861